2024-
2025

UNIVERSITY SYSTEM OF NEW HAMPSHIRE

STUDENT FINANCIAL SERVICES DATA PROTECTION PROTOCOL

USNH Student Financial Services Data Protection Protocol

Table of Contents

1. Purpose

The purpose of this protocol is to provide information handling standards that will ensure the protection of Restricted, Protected and Sensitive Information managed by USNH Student Financial Services (Regulated Data) from unauthorized access, loss or damage, while also supporting the effective operations of the Student Financial Services functions of the University System of New Hampshire and its component institutions (USNH).

Law, regulation and industry standards (including the Gramm-Leach-Bliley Act and the Payment Card Industry - Data Security Standard) require that USNH develop, implement, and maintain an information security program with administrative, technical, and physical safeguards designed to (1) ensure the security and confidentiality of Regulated Data, such as student financial aid-related information, (2) protect against any anticipated threats to the integrity of such information and (3) protect against unwarranted, unlawful and/or unauthorized disclosure, misuse, alteration, destruction or other compromise of such information, including unauthorized access to or use of such information that could result in substantial harm or inconvenience to any student. This Protocol applies to provide such safeguards for USNH records that are maintained on paper, electronically or by any other means.

2. Scope

This Protocol applies to all USNH employees, systems and networks involved with handling (including acceptance, transmission, storage, processing, retention and destruction) of Regulated Data. USNH policy requires that controls be in place to manage risk to the confidentiality, integrity, and availability of Regulated Data maintained in any form, and this Protocol represents a minimum standard for protection of such data.

3. Authority

The USNH Information Classification Policy details responsibilities for maintaining the privacy and security of institutional information, and assigns responsibility to Administrative, Academic, and Business Units to develop and maintain clear and consistent information handling procedures.

This Protocol accordingly supports:

- Adherence to USNH policies and legal requirements to maintain appropriate security controls for institutional information;
- Documentation of Student Financial Services practices and procedures; and
- Training for employees and others that handle Regulated Data in performing their roles.

Each USNH institution will designate a primary Student Financial Services Data Steward who will be responsible to implement this Student Financial Services Data Protection Protocol, and to address any questions or concerns that may arise relating to data security of Student Financial

Services records. Institutions will also designate a person of secondary responsibility who can act should matters arise when the primary Data Steward is unavailable. Data Stewards for the 2024-2025 Academic Year are:

- Keene State College
  Primary Data Steward - Cathy Mullins
  Secondary Data Steward – Fanny Kelly
- Plymouth State University
  Primary Data Steward - Mac Broderick
  Secondary Data Steward – Amy DelVecchia
- University of New Hampshire:
  Primary Data Steward - Elizabeth Stevens
  Secondary Data Steward - Jill Sikora

4. Revision

This policy may be updated at any time and is reviewed annually.

5. Definitions

Regulated Data includes any data managed by USNH Student Financial Services that is classified as Restricted Information, Protected Information or Sensitive Information under the USNH Information Classification Policy:

a. Restricted Information: Information is Restricted if protection is: legally defined; required by federal and/or state law (except FERPA records, which are Protected Data); required by contract or industry standard; or required by this Student Financial Services Data Protection Protocol. If compromised or exposed, Restricted information could result in significant institutional cost, harm to institutional reputation, and/or unacceptable disruption of the institution's ability to meet its mission. Examples of data that Student Financial Services manages that is designated as Restricted Information include:
   - Social Security Numbers
   - Tax Information, including applicant and contributor information covered by section 483(a)(3)(E) of the Pre -FUTURE Act / FAFSA Simplification Act
   - Non-public, personally identifiable financial information, as defined in the Gramm-Leach-Bliley Act
   - Bank account numbers and routing information
   - Student account data and loan information

b. Protected Information: Information is Protected if privacy controls are required by regulation or law but required protections do not rise to the level of those mandated for Restricted Information. Compromise or exposure of Protected Information may result in serious institutional cost, harm to institutional reputation, and/or unacceptable disruption

of the institution's ability to meet its mission. Examples of Protected Information typically managed by USNH Student Financial Services include:

- Financial assistance records that are not considered non-public personally identifiable financial information
- Budgets and salary information
- Disciplinary records
- Student educational records, including academic transcripts and other scholastic records

c. Sensitive Information: Information is Sensitive if controlled access is required by institutional policy, by this Student Financial Services Data Protection Protocol, by contract, for ethical reasons, and/or if it is at high risk of damage or inappropriate access. Sensitive Information includes information which, if compromised, could result in high institutional cost, harm to clients, harm to institutional reputation or unacceptable disruption of the institution's ability to meet its mission. Sensitive Information requires controlled access, but does not require the level of data security protection dictated for Restricted or Protected Information. Any information that has not been designated Restricted, Protected or Public Information is considered Sensitive Information. Examples of Sensitive Information that is often managed by USNH Student Financial Services include:

- University ID numbers (**except,** if USNHID is used in conjunction with other personally-identifying data elements it is designated as Protected Information)
- Directory information
- Intellectual property
- Fundraising data

6. Data Access Management

Access to Regulated Data is restricted to those users who need such information to perform their jobs. Each institution's Student Financial Services Data Steward will maintain current lists of employees with access to the various Student Financial Services records management systems, and will review the list periodically to ensure that the list reflects the most current access needed and granted. When possible, these lists should be maintained as a record that is saved within the administrator profile of the applicable record management system. If access to a list is requested for audit purposes, the appropriate Student Financial Services Data Steward will access and provide that list.

Privileges to access records managements systems that contain Regulated Data are to be assigned to individuals based on job classification and function, as determined by the Student Financial Services Data Steward for each institution. Any individual who is provided with such privileges is subject to a background check, paid by the University System of New Hampshire and managed through the campus Human Resources/ Recruiting office. Supervisors must provide prompt notification of an employee's termination or other removal of authorized access to Regulated Data, using the USNH client portal ticket request.

7. General Data Security Procedures

a. All personnel who have access to Student Financial Services records must abide by general best practices in management of Regulated Data, including removal or redaction of Restricted Information or personally identifiable information (PII) whenever possible if it is not needed for business purposes.

b. In accordance with the USNH IT Access Management Standard, employees may not use anyone else's USNH account or allow others to use their passwords or account access.

c. Employees must remove Regulated Data from desktops and any areas of public access such as tables, printers, copiers and fax machines. Offices containing Regulated Data must be locked at night or when otherwise not in use. Paper records containing Regulated Data must be stored in locked file cabinets in restricted access areas. Keys or access badges for rooms or file cabinets containing Regulated Data must be properly secured to prevent access by unauthorized personnel.

d. Discretion must be used when discussing Regulated Data over the phone, to ensure it is not overheard.

e. Authorized employees who access Regulated Data from an external network using remote access solutions must comply with the USNH IT Remote Access Security Standard.

f. All Restricted and Protected Information must be protected by encryption both in transit over external networks and at rest, unless such protection is infeasible and the USNH CISO approves alternative compensating controls.

g. Multi-factor authentication is required for any individual accessing Student Financial Services information systems, unless the USNH CISO approves in writing the use of reasonably equivalent or more secure access controls.

8. Acceptance and Handling of Data

Employees must observe the following procedures when accepting and handling Regulated Data.

a. Acceptance of Regulated Data
   - Employees must only accept Regulated Data that is within their data access privileges, and should refer the matter to an authorized employee if they are presented with data that is outside of their access privileges.
   - Designated secure fax and copiers should be used for acceptance and transmission of Restricted Information or Protected Information.
   - Any Restricted Information or Protected information received via paper mail should be scanned and saved to electronic databases and then set for secure shredding within 48 hours.

b. Transmission of Regulated Data

- If other USNH departments or employees have been approved to receive Restricted or Protected Information, it should be sent and accessed when possible through USNH systems (i.e., Banner/Xtender, Slate, Webi, SharePoint, Workday) rather than email.
- Regulated Data may not be transmitted by IM, text or voicemail.
- Restricted Information and Protected Information may not be sent by unencrypted email.
- When sending Restricted Information by mail (including U.S. Postal Service, DHL, UPS, FedEx, etc.), the sender must obtain secure, certified, tracking and signature confirmation services and use a tamper-evident sealed package. It is highly recommended that obfuscation or encryption of the sensitive data items be done prior to mailing.
- Where feasible, alternatives to mail delivery should be utilized such as a secured, encrypted online transmission. Transmissions that utilize passwords to encrypt or decrypt data must have their own unique identifier or password.
- Restricted Information may not be released over the phone. Before releasing Protected or Sensitive Information to a student, parent or guardian over the phone, employees must verify the caller's identity. To verify identity, staff should have the caller verify multiple pieces of the following information:
    - Student First Name and Last Name
    - Parent/Guardian First Name and Last Name
    - Student DOB
    - Student UNHID
    - A phone number on the record
    - Student home address
    - Last four numbers of Student Social Security number

c. Storage of Regulated Data

- Student Financial Services records are created in the normal course of conducting business, and must be appropriately and securely stored throughout their entire life cycle in order to document the decisions and activities of complex educational and business processes.
- Student Financial Services records containing Regulated Data should exist only in areas where there is a legitimate and justifiable need.
- Employees are not permitted to take Regulated Data off campus or to make unofficial copies, except with written authorization by the institutional Student Financial Services Data Steward.
- Regulated Data may not be stored on any unencrypted device.
- Restricted or Protected Information may not be stored on portable electronic media devices (including laptops, disks, flash drives, portable hard drives).
- Restricted or Protected Information may not be stored on personal mobile devices. Employees who have a valid need to store other non-public data on such devices must seek guidance regarding additional controls from the appropriate Student Financial Services Data Steward and/or ET&S Cybersecurity.

9. Data Retention and Destruction

Student Financial Services records, in any format, will be retained and destroyed as detailed in the records retention schedule attached as Appendix 1 to this Protocol. Non-public, personally identifiable financial information will be retained no later than two years after the last date the information is used in connection with the provision of a product or service to the customer to which it relates, unless such information is necessary for business operations or for other legitimate business purposes, is otherwise required to be retained by law or regulation, or where targeted disposal is not reasonably feasible due to the manner in which the information is maintained.

Record retention schedules will be reviewed periodically to minimize unnecessary retention of data.

All paper records containing Regulated Data must be disposed of by secure shredding. In the event of any recycling of computers containing Regulated Data, all memory components of such computers will be completely reformatted or otherwise erased for any new use as determined by USNH ET&S.

10. Responding to a Data Security Breach

A data breach is any instance in which there is an unauthorized release or access of Regulated Data. This definition applies regardless of whether the data is stored and managed directly by Student Financial Services or through a contractor (e.g., cloud service providers). Data breaches can take many forms including: malicious attacks by hackers; lost, stolen, or misplaced equipment (e.g., laptops, mobile phones, portable thumb drives, etc.); unauthorized access or failure of data protocols through negligence (e.g., leaving a password list in a publicly accessible location, technical staff misconfiguring a security service or device).

Any employee who suspects that a data breach may have occurred must immediately notify their supervisor and the IT Help Desk:

KSC: (603) 358-2532
PSU: (603) 535-2929
UNH: (603) 862-4242

In the event of a suspected data breach, Student Financial Services must immediately execute each of the relevant steps outlined below, in addition to following applicable USNH or institutional incident management procedures:

a. Document every action you take from the point of suspected breach forward, preserving any logs or electronic evidence available. Include in the documentation:
   - Date and time
   - Action taken
   - Location

- Person(s) performing action
- Person(s) performing documentation
- All personnel involved

b. Contact USNH ET&S Cybersecurity and the departmental IT or Information Security Office for proper direction of preservation of electronic data. The steps should include:
   - Disconnect the computer/device(s) from the network. To disconnect the device from the network, simply unplug the Ethernet (network) cable, or if the device uses a wireless connection, disconnect it from the wireless network.
   - DO NOT turn the device off or reboot. Leave the device powered on and disconnected from the network.

c. Prevent any further access to or alteration of the compromised system(s). For example, do not log on to the machine, change passwords or run a virus scan). In short, leave the system(s) alone, disconnected from the network, and wait to hear from a security consultant.

d. If a suspected or confirmed intrusion/breach of a system has occurred, the Data Steward, in connection with USNH ET&S, will alert USNH Internal Audit, USNH General Counsel, and the appropriate institutional Vice President.

e. USNH Student Financial Services employee lapses will be logged and resolved; lapses are defined as cases where employees did not follow correct procedure, but which did not result in a security breach. Employees who do not comply with this policy will be re-trained, and are subject to sanctions, including loss of computer or network access privileges, disciplinary action, suspension and termination of employment, as well as legal action.

11. Training

Employees must complete all cybersecurity training required for their role, consistent with the USNH Training Standard. Such trainings may include: GLBA Cybersecurity Training, PCI-DSS Compliance Training, HIPAA Compliance Training, Advanced Cybersecurity Training, and/or Cybersecurity Incident Response Training. Upon completion of required training, supervisors will ensure that employees who handle Regulated Data as part of their employment or other activity at USNH fill out and sign applicable employee statement of understanding forms, which will be saved and stored with the department director.

12. Data Security Policies and Standards

Additional controls required under applicable laws, regulations, or standards governing specific forms of data (e.g., health information, credit cardholder data, student records), may also apply. USNH resources provide guidance on safeguards for specific Regulated Data:

a. Material Transfer Agreements (MTAs)

b. Family Educational Rights & Privacy Act records (FERPA)
c. Health Insurance Portability & Accountability Act (HIPAA)
d. Payment Card Industry - Data Security Standard (PCI-DSS)
e. Gramm Leach Bliley Act (GLBA)
f. General Data Protection Regulation (GDPR)
g. Controlled Unclassified Information (CUI)
h. Export Controls
i. Confidentiality or Non-Disclosure Agreement (CDA or NDA)

Additional guidance on data security can be found in the USNH Technology /Cybersecurity Policies & Standards.

Protocol Effective Date: October 1, 2024
Approved by: GLBA CC
Reviewed by: FINEC
Revision History:

Appendix 1 - Student Financial Services Data Retention Schedule

Responsibilities

Each Student Financial Services Data Steward is responsible for managing data retention and destruction within their department consistent this retention schedule and USNH Financial Records Retention Periods

Procedures

Each Student Financial Services Data Steward, or a designee, must:

- Determine the appropriate format for retention of records under their area of responsibility;
- Implement record management practices that are consistent with this policy;
- Educate staff within their area of responsibility in understanding sound record management practices;
- Ensure preservation of records that are of historic value, and transfer those records to the University Archives;
- Ensure preservation of all other records consistent with their applicable retention period;
- Destroy University records that have no active or archival value upon passage of the applicable retention period.
- When the prescribed retention period (see the Record Retention Table) for a record has passed, they should ensure that the records are properly disposed of unless the records are of archival value to the University.
- Disposal of records must be suspended if (1) litigation or federal or state investigation has commenced or is threatened, or (2) the USNH General Counsel's office has determined that circumstance require the preservation of records.

USNH Document Retention Schedule for Student Financial Aid Records

	Minimum Retention Period
Records related to school eligibility	
Program Participation Agreement, approval letter, and Eligibility and Certification Approval Report	3 years from the end of the award year
Application portion of the FISAP	3 years from the end of the award year
Accrediting and Licensing agency reviews, approvals, and reports	3 years from the end of the award year
State Agency reports	3 years from the end of the award year
Audit and program review reports	3 years from the end of the award year
Self-evaluation reports	3 years from the end of the award year
Financial Responsibility and Administrative Capability records	3 years from the end of the award year
Records related to student eligibility	
Cost of attendance	3 years from the end of the award year
Documentation of a student's Satisfactory Academic Progress	3 years from the end of the award year
Documentation of a student's program of study and the courses in which the student enrolled	3 years from the end of the award year
Data used to establish student's admission, enrollment status, and period of enrollment Required student certification statements and supporting documentation	3 years from the end of the award year
Documents used to verify applicant data and resolve conflicting information	3 years from the end of the award year

Documentation of all professional judgment decisions	3 years from the end of the award year
Financial aid history information for transfer students	3 years from the end of the award year
Student Aid Report or Institutional Student Information Records	3 years from the end of the award year
Fiscal Records	
FSA program transaction records	3 years from the end of the award year
Bank Statements for all accounts containing FSA funds	3 years from the end of the award year
Records of student accounts	3 years from the end of the award year
General ledger that identify each FSA program transaction	3 years from the end of the award year
Federal Work Study payroll records	3 years from the end of the award year
The fiscal operations portion of the FISAP	3 years from the end of the award year
Data for required FSA program reconciliation reports	3 years from the end of the award year
Pell Grant statements of accounts	3 years from the end of the award year
Cash requests and G6 reporting	3 years from the end of the award year
Audit reports and school responses	3 years from the end of the award year
State grant and scholarship award rosters and reports	3 years from the end of the award year
Aid Specific Program Records	
Direct loan borrower eligibility records (loan certification, SAI, cost of attendance, MPN, Entrance Counseling)	3 years from the end of the award year in which the student last attended.

Disbursement dates and amounts	3 years from the end of the award year in which the student last attended.
Perkins Loan repayment records	3 years from the date the loan was assigned to the Department, cancelled, or repaid.
Perkins Loan original promissory note	Until the loan is satisfied or needed to enforce the obligation.
Application data submitted to the Department or the school on behalf of the student	3 years from the end of the award year
FWS payroll disbursement information	3 years from the end of the award year
FWS certification by the student's supervisor of hours work/paid	3 years from the end of the award year
SEOG disbursement documentation	3 years from the end of the award year
Documentation of refund calculations	3 years from the end of the award year